AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kathryn I. Murray, a Special Agent with Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices known as a Black Lenovo ThinkPad bearing S/N: PC – 09V99D with charger, Silver in color Hard Drive bearing S/N: ZL203YCS and Silver in color Hard Drive bearing S/N: ZJV01ALG, hereinafter the "SUBJECT DEVICES," further described in Attachment A, for the items described in Attachment B.

2. Since August of 2004, I have been a Special Agent with Homeland Security Investigations ("HSI"), assigned to the Resident Agent in Charge ("RAC") Allentown, Pennsylvania Office, which is under the Special Agent in Charge in Philadelphia, Pennsylvania. My duties include the investigation of criminal violations, including violations related to child exploitation and child pornography offenses, such as the production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including digital media. My duties also include the investigation of offenses involving the transportation with intent to engage in criminal sexual activity, and travel to engage in in illicit sexual conduct, in violation of 18 U.S.C. §§ 2423(a) and (b).

3. I have also participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2423, among others, and I am authorized by law to request a search warrant.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct), 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct), and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), are presently located at the SUBJECT DEVICES.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any

means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

b. Title 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually

explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A

password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

i. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Mobile application" or "chat application," as used herein, are specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, digital, or magnetic form.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal.

1986), *aff'd sub nom*, *United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *aff'd*, 813 F.2d 1231 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987)

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON PEER-TO-PEER NETWORKS

7. Your affiant knows through training and experience one of the fast-growing areas that facilitates and is used by Child Sexual Abuse Material collectors and traders is peer-to-peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. The P2P Networks, such as such as FastTrack, eDonkey, BitTorrent, Ares, UTorrant, and the Gnutella have become ideal for traders to openly exchange collections and share those collections. The P2P network has provided a way for traders to have what they feel is an open and anonymous distribution and trading network. This network enables trading on a world-wide basis and with upload and download speeds as if the trader was next door.

8. Your affiant knows that computers on these networks have software installed on them that facilitate the trading of images. The software, when installed, allows the user to search

for pictures, movies and other digital files by entering text as search terms. Some names of the software used include, but are not limited to, eDonkey, BearShare, Frostwire, LimeWire, Shareaza, Morpheus, Gnucleus, Phex and other software clients.

9. P2P file sharing networks are frequently used to trade digital files of Child Sexual Abuse Material. These files include both image and movie files. P2P file sharing programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files.

10. Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

11. To access the P2P networks, a user first must purposely seek out P2P software for sharing on the internet and then obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide P2P network for download. Most P2P software gives each user a rating based on the number of files he/she is

contributing to the network and on the user's bandwidth and firewall settings. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is not required to share files to utilize the P2P network. P2P programs are able to communicate with other P2P programs. For example, a user utilizing the BitTorrent network is able to communicate with a user on a different network, such as UTorrant.

12. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, information about the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then purposefully selects file(s) which he/she wants to download. There is no accidental download process. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event.

13. Thus, a person interested in sharing Child Sexual Abuse Material with others in the P2P network, need only place those files in his/her "shared" folder(s) or leave the files they download in the shared folder. Those Child Sexual Abuse Material files are then available to all users of the P2P network for download regardless of their physical location.

14. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time thus speeding up the rate at which a single file is downloaded. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The user's computer then reassembles those parts into the single file. This reduces the time it takes to download the file. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular Internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

15. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to forcefully send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload Child Sexual Abuse Material files to another user's computer without his/her computer's active participation.

16. The investigation of peer-to-peer (P2P) file sharing networks is a cooperative effort of law enforcement agencies around the country. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing Child Sexual Abuse Material, some of which were also involved in the active sexual exploitation of actual child victims.

SUMMARY OF INVESTIGATION

17. In January of 2024, Kathleen Fallon, a Special Agent with the Pennsylvania Office of Attorney General ("PA OAG"), reviewed recent downloads from a law enforcement BitTorrent file sharing program. At this time, SA Fallon found multiple files downloaded and shared by a BitTorrent user utilizing IP address 64.121.160.13 that consisted of child sexual abuse material ("CSAM"); that is, images of children under the age of eighteen engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2). These downloads occurred between January 08, 2024, at 18:04:16 UTC and January 9, 2024, at 06:40:29 UTC.

18. On January 08, 2024, at 18:04:16 UTC and January 9, 2024, at 06:40:29 UTC, the law enforcement BitTorrent program was able to download from IP address 64.121.160.13 a folder named "Julyjailbait.club." This folder contained over one hundred (100) images of CSAM. Sixty-six (66) of those images were contained in a sub-folder labeled "BDSM." One file within that sub-folder was named 14857343.jpg. This file depicts an image of a female infant, between the ages of three (3) months and nine (9) months old. This infant is nude and is being posed by an adult male to show her genitals to the viewer. The male is using his hand to place a plastic hair clip on the infant's vagina.

19. SA Fallon viewed all the images in the "BDSM" sub-folder, and this folder contains over sixty-six (66) images of CSAM. Almost all images depict children under the age of 11 years old, engaged in sexual acts while being restrained by ropes, collars, and other devices. The youngest child depicted in these images appears to be between three (3) months and nine (9) months old.

20. The next file name in the "JulyJailbait.club" folder is labeled "Pedomom." This folder contains over one hundred (100) images of CSAM depicting children as young as three (3) months old. One file name "felixxx_062205vg_20050601082847R.jpg" depicts a nude adult female laying on her back and holding up a nude infant female. The adult female has her tongue out and penetrating the female infant's vagina. This infant appears to be three (3) to six (6) months old.

21. The final file name in the "Julyjailbait.club" folder is labeled "zoo." This file contains over 18 images of children performing sexual acts with animals. One file name "felixxx_100643RL2_itekanRs.jpg," is an image that depicts a female infant who is nude laying with on her back with her shirt pushed up to her chest, exposing her vagina. While laying on her back, a black and brown dog is licking her vagina. The female infant appears to be between three (3) and five (5) months old.

22. All the images contained in "JulyJailbait.club" are classified by the National Center for Missing and Exploited Children ("NCMEC") as "known CSAM images/videos." Additionally, SA Fallon viewed the photos shared by IP address 64.121.160.13 within the folder and confirmed that all photos in this folder depicted CSAM as defined under 18 U.S.C. § 2256(8).

23. All of the aforementioned images of CSAM were shared by a device utilizing IP address 64.121.160.13 and operating the BitTorrent file sharing program between January 08, 2024, at 18:04:16 UTC and January 09, 2024, at 06:40:29 UTC.

24. On January 31, 2024, SA Fallon utilized a publicly accessible website that shows what internet provider is assigned to a specific IP address. As a result of this search, it was found that Astound Broadband, LLC maintains this IP address and is owned by RCN Telecom Services,

LLC. On this same date, SA Fallon submitted an administrative subpoena to RCN Telecom Services, LLC for the subscriber information pertaining to IP address 64.121.160.13 for January 08, 2024, at 18:04:16 UTC and January 9, 2024, at 06:40:29 UTC.

25. On February 6, 2024, SA Fallon reviewed the response from RCN Telecom Services. The following subscriber information was obtained:

Account Number: 39056545904

Subscriber Name: WEI FU

Subscriber & Billing Address: 1924 VINTAGE DR. EASTON, PA 18045-5405

Length of Service: 06/23/2021 - Currently Active

Associated Email Addresses: wfu0l@hotmail.com

Associated Phone Numbers: 201-360-1833

26. On February 27, 2024, SA Fallon arrived at 1924 Vintage Dr. Easton, Northampton County, PA 18045. This residence is a two-story single home, tan in color with dark shutters. The numbers "1924" are printed in large gold on the front door or the residence. The PA OAG Intelligence Unit confirmed through the PA Department of Transportation records that Wei Fu resides at this residence.

27. On March 6, 2024, SA Fallon applied for a Pennsylvania search warrant for 1924 Vintage Dr. Easton, Pa 18045. This warrant was signed by Magisterial District Judge Sandra McClure. On March 7, 2024, Agents from the Pennsylvania Office of Attorney General, Homeland Security, and detectives from the Bethlehem Township Police Department executed this warrant at 1924 Vintage Dr. Easton, PA 18045.

28. On scene, agents and detectives contacted one individual inside this residence. This individual was later identified as Wei Fu. Law enforcement informed FU that they had a search warrant for the residence and for all electronic devices. After securing the residence, law enforcement asked FU if he would speak with law enforcement and apprised him that the conversation would be audio and video recorded. FU consented to an interview. SA Fallon informed FU of his rights per *Miranda*. SA Fallon read the PA OAG *Miranda* form to him and gave him an opportunity to read the form. FU then signed the form and stated he understood. PA OAG SA Brian King and Homeland Security SA Kathryn Murray were present during this interview. While speaking with FU, we learned that he is the sole occupant of 1924 Vintage Dr. Easton, PA 18045. FU stated that he has been living alone at this residence since 2020. FU stated he is a software engineer for Cox Automotive Corporation and that he works from home. FU stated that his work computer is an Apple MacBook, and it was in his bedroom. FU also stated that he has multiple personal computers in his bedroom. SA Fallon informed FU that we are investigating illegal internet activity. When SA Fallon asked him what illegal internet activity was and what we were looking for, FU stated the illegal activity would be pornography. When SA Fallon asked FU if we would find child pornography on any of his devices, he stated that we would find child pornography on his personal computer. FU stated that his current internet service provider is RCN Telecom Services.

29. During this interview, FU stated that he uses peer to peer file sharing programs to download child pornography, specifically UTorrant. SA Fallon asked FU if he understands how peer to peer file sharing works and he stated that he did. He stated that he knows that he is downloading other UTorrant user's files and also sharing his own files. FU stated that he believes

he has set his UTorrant not to share files, but not all the time. SA Fallon asked FU what search terms he uses to find the child pornography and he stated that he would just use the term "child pornography." FU stated that he started viewing child pornography in the last year because he was bored with adult pornography. FU stated that he was just curious about the child pornography. FU stated that the youngest child he has seen depicted in the videos and images was 10 years old. SA Fallon informed FU that she had recent downloads depicting children as young as three (3) months old engaged in sexual acts and being restrained by ropes and other devices. FU stated that when he downloads his child pornography, it downloads a large package of all kinds of child pornography, and he didn't have time to go through all the files he has. SA Fallon asked FU if he was sexually attracted to children and he stated the wasn't, he was just curious. SA Fallon asked FU if he wasn't attracted to children why did he keep such a large collection of child pornography and he stated that he just likes to collect stuff. SA Fallon informed FU people collect stuff that they like and are interested in, and he stated he understood that.

30. While speaking with FU, PA OAG forensics agent performed an on-scene preview of FU's electronic devices, including personal computers and cell phones. Supervisory Special Agent ("SSA) James McDonald informed SA Fallon that they had located the UTorrant file sharing program on FU's personal computer. SSA McDonald also stated he located over fifty (50) images and videos of children that were nude and engaging in sexual acts. These children were all under the age of eleven (11) and engaging in sexual acts including penetration and attempted penetration. SA Eric Barlow informed SA Fallon that he was also conducting a preview of a hard drive found in FU's personal computer. He stated that the hard drive only contained adult pornography and a series of photos that were difficult to determine age. SSA McDonald stated the

hard drive he was previewing only contained child pornography. Both hard drives were seized along with a Lenovo Laptop by the PA OAG. SSA McDonald conducted an initial forensic examination of these devices which resulted in the discovery of both images and videos of child sexual abuse material (CSAM).

31. On June 4, 2024, your affiant took custody of the SUBJECT DEVICES and entered the three into evidence at HSI Philadelphia, PA.

32. On June 28, 2024, your affiant reviewed the initial forensics results generated by SSA McDonald and discovered approximately 4,500 images of CSAM. A sample of the images are described below:

a. File Name: 0100.jpg is an image of a prepubescent female tied to a bed with purple sheets and white flowers. The female, who appears to be Filipino, is wearing a blue skirt with matching shirt. The female, who is approximately 5 to 7 years of age, is bound with white rope at her ankles and wrists. The female's legs are spread exposing her vagina. (Created Date: 5/28/2024 9:31:46 AM)
b. File Name: 0117.jgp is an image of a prepubescent female being vaginally penetrated by an unknown white male's erect penis. This is the same female from image 0100.jpg. (Created Date: 5/28/2024 9:31:46 AM)

Additionally, your affiant discovered approximately 550 videos of CSAM. A sample of the videos are described below:

c. File Name: (Pthc[1])!!! New 0604 !!! Luvnlilly 3Yo(1).avi is a video of a prepubescent female, who is approximately 2 to 4 years of age. The video appears to be a compilation video of the same prepubescent female. An unknown male places the female's hands on his erect penis and assists her with masturbation. At approximately 1 minute and 49 seconds into the video, the unknown male masturbates to completion on the female's chest and stomach. At approximately 5 minutes and 36 seconds into the video, the female appears to be asleep and the unknown male places his erect penis in between her legs and begins to masturbate using her legs. The female is wearing a plaid skirt with no shirt and does not have on underwear. The male masturbates to completion on the female's legs. The video is 7 minutes and 30 seconds in duration. (Created Date: 5/28/2024 9:30:55 AM)

[1] I know from my training and experience that "Pthc" is a common abbreviation used by those who save child pornography files and stands for pre-teen hard core.

d. File Name: 6yo_daughter_fuck.mp4 is a video that opens with the following title screens "Blue Diamond Productios Present" and "6YO Doughter Penetration." The video is of a prepubescent female wearing a denim skirt that is lifted, a pink shirt and a pair of pink underwear that are removed and still on her right leg. The female is being vaginally penetrated by an unknown white male's erect penis. There is music playing in the background of the video and a blue diamond logo is on the right side of the screen. The video is 5 minutes in duration. (Created Date: 5/28/2024 9:38:23 AM)

33. On July 9, 2024, FU was indicted in the Middle District of Pennsylvania in violation of 18 U.S.C. 2252(a)(2) (distribution of child pornography – 1 count). FU was arrested without incident on July 11, 2024.

34. Additional forensics are needed to fully analyze and review the SUBJECT DEVICES and will be completed by Computer Forensics Agent/Special Agent James Munjone with Homeland Security Investigations. SA Munjone will reimage the SUBJECT DEVICES and process the evidence utilizing Griffeye Pro, a forensic tool that PA OAG did not utilize during its review. Griffeye Pro is a forensic tool that allows for the processing, sorting and analyzing of large volumes of image and video files.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

35. As described in Attachment B, this application seeks permission to search for images, videos, and records that might be found on the SUBJECT DEVICES, in whatever form they are found. One form in which these items might be found is data stored on a computer's hard drive, mobile device, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic devices and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. I submit that if a computer[2] or storage medium is found, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system

[2] Anytime the term "computer" is used in this affidavit, it's definition includes mobile devices such as mobile telephones. See ¶ 6(d) above.

configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may

provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend

on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

34. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or

months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

d. Furthermore, the electronic media may contain contraband, in the form of images and videos depicting the sexual exploitation of minors.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE AND POSSESS CHILD PORNOGRAPHY

37. Based on my education, training, and experience, as well as information obtained from other experience law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce and possess child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual

media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including, but not limited to print and digitized/electronic media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain this material for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still

discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Based on the investigation to date, FU is an individual who has possessed child pornography.

38. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-

based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

CONCLUSION

39. Based upon the information above I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct), 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct), and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) have been committed and that evidence of those violations is located on the SUBJECT DEVICES. This evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the SUBJECT DEVICES identified in Attachment A, for the items listed in Attachment B.

_/s/ Kathryn I. Murray_____
Kathryn I. Murray
Special Agent
Homeland Security Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on August 30, 2024.

Pamela A. Carlos

Digitally signed by Pamela A. Carlos
Date: 2024.08.30 10:53:21 -04'00'

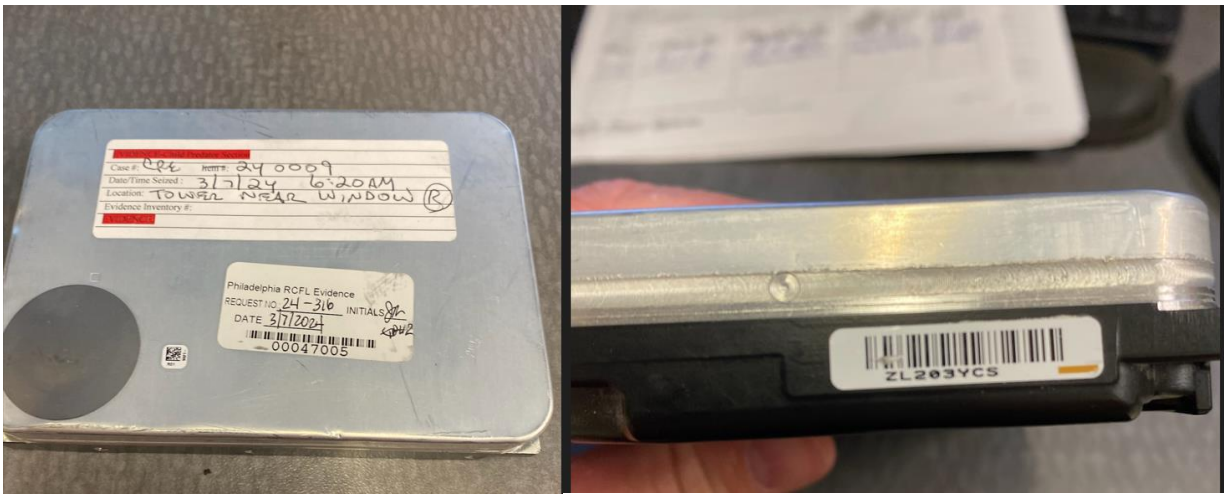
HONORABLE PAMELA A. CARLOS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF DEVICES TO BE SEARCHED

1. Black Lenovo ThinkPad bearing S/N: PC – 09V99D (with charger)

2. Silver in color Hard Drive bearing S/N: ZL203YCS



3. Silver in color Hard Drive bearing S/N: ZJV01ALG

All of the above devices are currently located in secure evidence storage at Homeland Security Investigations/SAC Philadelphia Office.

ATTACHMENT B

DEVICE TO BE SEARCHED FOR AND SEIZED

Evidence of violations of 18 U.S.C. Section 2252 including the following:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened e-mails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.

3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

7. Documents and records regarding the ownership and/or possession of the subject device.

8. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

9. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

10. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

11. The following may be seized and searched for all items listed above, and for any items specifically noted in the paragraphs below:

a. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of Internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, wireless routers, cables and connections, web cameras, microphones); storage media, defined below; and security devices, also defined below.

b. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

c. Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

d. Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or date or to otherwise render programs or data into usable form.

e. All storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, ipods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.

The above seizure of computer and computer related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. Upon a determination that such examination would be more appropriately made in a controlled environment, this storage media may be removed and examined at a laboratory location.